ECKERT SEAMANS ATTORNEYS AT LAW

December 17, 2024

Cybersecurity, Data Protection & Privacy Update

A Must Have New Years Resolution for Covered Entities: Completing a HIPAA Risk Analysis

By Matthew H. Meade, Elizabeth Wilson, Laura A. Decker & Gregory P. Mazmanian

WHY IT IS IMPORTANT TO COMPLETE A HIPAA RISK ANALYSIS

As the year comes to a close, the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR"), the division within HHS tasked with enforcing the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), released a number of resolution agreements against covered entities. Resolution agreements are settlements or penalties arising from OCR HIPAA security rule and/or privacy rule compliance investigations. As of December 10, OCR issued fourteen (14) monetary penalties/settlements over the course of 2024, with five (5) announced in the last couple of months.[1] Please see the "*Recent OCR Penalties*" section below for a summary of the five most recent penalties imposed by OCR.

The common thread throughout those five penalties is the covered entity's failure to conduct a HIPAA-compliant risk analysis.[2] This OCR enforcement uptick may be due to OCR's recent rollout of its "Risk Analysis Initiative", which was created to address the 264% increase in large data breaches seen by OCR since 2018.[3] For further information on OCR's recent Risk Analysis Initiative, please see our previous client alert. Given the release of this new OCR initiative, non-compliant covered entities should be prepared for increased scrutiny and higher likelihood of fines from OCR in 2025.

WHAT IS A HIPAA RISK ANALYSIS?

General Requirement

The risk analysis is an essential component of a HIPAA covered organization's strategy for protecting electronic protected health information ("ePHI"), and a requirement under the HIPAA Security Rule. In response to the recent rise of enforcement actions based in part or in whole upon noncompliance with this administrative safeguard, it is essential for an organization to understand what OCR expects from the risk analysis process. The text of HIPAA's risk analysis requirement states that a covered organization must:

> "*Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [ePHI] held by the covered entity.*"[4]

In practice, this means covered entities must: (i) review and identify potential security risks to ePHI and (ii) determine the likelihood these risks will occur as well as the risk's degree of impact to ePHI.[5] There is no single risk analysis

[1] *See* HHS Resolution Agreements and Civil Money Penalties, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
[2] *See* 45 CFR § 164.308(a)(1)(ii)(A).
[3] U.S. Department of Health and Human Services (HHS), *HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation for $90,000*, October 30, 2024 ("OCR Risk Analysis Initiative Enforcement Action").
[4] 45 C.F.R. § 164.308(a)(ii)(A).
[5] *See HIPAA Security Series 2* at 4.

framework that provides absolute compliance with the Security Rule requirements. However, two key steps to complete a risk analysis includes (i) completing an ePHI data map and (ii) identifying risks to the organization's ePHI as well as potential mitigation measures to address these risks.

Data Mapping

The Security Rule requires covered entities to complete a risk analysis that encompasses the "potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that an organization creates, receives, maintains or transmits."[6] As such, an organization must identify all the ePHI that is transmitted, received, created or maintained by the organization and must document the results of this process. To identify all potential sources of ePHI, an organization must consider less traditional data repositories, such as portable devices (e.g., phones or tablets) and ePHI held by third parties, such as vendors or partner organizations.

Risk Identification & Mitigation Measures

Once an organization has identified its sources of ePHI and where that data resides in its systems, it must also identify and document reasonably anticipated threats to its ePHI, and vulnerabilities which would create a risk to the confidentiality, integrity, and availability of its ePHI. This includes sources of human, natural, and environmental threats to an organization's systems that contain ePHI. A covered entity should also assess and document the likelihood of impact related to each identified threat to their ePHI and the strength of the assigned risk level (i.e., the "criticality") of the identified risks to the organization's ePHI. Additionally, risk analysis documentation should include mitigation actions to be taken by the subject organization in response to the identified threats.

Risk Analysis Documentation and Periodic Review

The Security Rule requires covered entities to document their risk analysis. However, HIPAA does not specify the format of such documentation, so organizations have flexibility in how they wish to document their risk analysis. Covered entities also have an ongoing obligation under the Security Rule to periodically review and update the risk analysis, and to document any changes, to ensure reasonable and appropriate protection of the ePHI they maintain. Please note that HIPAA does not specify the frequency for these periodic reviews, and OCR acknowledges that review frequency may "vary among covered entities" and be conducted "annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment".[7]

For further guidance on the HIPAA risk analysis requirements, OCR developed a webinar and practical guidance to assist covered organizations.

RISK ASSESSMENT TOOL ("SRA TOOL") FOR SMALL / MEDIUM SIZED COVERED ENTITIES

How to Access the SRA Tool

OCR, in collaboration with the Office of the National Coordinator for Health Information Technology (ONC), developed a "Security Risk Assessment Tool" ("SRA Tool") to help small and medium sized covered entities comply with the risk analysis requirement. Small and medium sized entities should take note that there is no charge associated with using the SRA Tool. Covered entities should note that the SRA Tool includes a legal disclaimer stating that using the SRA Tool does not guarantee HIPAA compliance and may not be appropriate for all covered entity types.[8] Covered entities

[6] *See OCR Risk Analysis Guidance.*
[7] *See OCR Risk Analysis Guidance.*
[8] *See* https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool for full legal disclaimer.

can download Version 3.5 of the SRA Tool to a Microsoft Windows computer (an excel version of the SRA Tool is available for those who do not have Windows). The SRA Tool assessment is highly detailed and may take several hours to complete, however it should not take weeks to complete if the entity has a good understanding of its security programs. The assessment can be saved and re-visited later if needed. Please note that per the SRA Tool guide, the SRA tool is a local application, and no information and/or reports generated using the SRA Tool is sent to OCR or ONC or is otherwise transmitted over the Internet.[9] Guidance on how to navigate the SRA tool is located in the SRA Tool User Guide.

Completing the SRA Tool Assessment

Once downloaded, the covered entity will be guided through seven (7) sections covering the following HIPAA security topics: (i) risk analysis requirements, (ii) security policies, (iii) workforce security, (iv) technical security measures, (v) physical security measures, (vi) business associates, and (vii) contingency planning. Each section includes a list of multiple-choice questions along with open text boxes to allow covered entities to provide further detail or clarity on their answers. The SRA Tool should be completed by the HIPAA Security Officer and someone familiar with the organization's IT infrastructure.

At the end of each section there is a list of threat/vulnerability main categories and sub-categories that the covered entity can select as relevant to their organization. If a covered entity selects a particular threat/vulnerability, they will need to assign a risk level to the threat/vulnerability by indicating: (i) the threat/vulnerability's likelihood of occurring (i.e., "low, medium, or high") and (ii) the relative impact the threat/vulnerability would have on the covered entity if the threat occurred (i.e., "low, medium, or high").

SRA Tool Output

After each section, a "section summary" is generated which details areas of the covered entity's security program that meets expectations ("areas of success") and needs improvement ("areas for review"). After the assessment is completed, the covered entity will receive a "security risk assessment summary" and three reports (a "detailed report", a "risk report", and a "remediation report"), which are further discussed below. If the organization flagged questions to be answered later, the organization can also generate a "flagged report" which provides a list of all flagged questions.

- The "*security risk assessment summary*" provides a snapshot of the organization's overall risk level by providing (i) an overall risk score percentage as well as risk score percentages for each of the seven sections, (ii) the number of identified areas for reviews that will need to be addressed, (iii) the number of identified organization vulnerabilities.
- The "*risk report*" includes (i) a breakdown percentage for each of the organization's identified risk ratings (i.e., the percentage of low, medium, high, and critical risks identified), (ii) each of the organization's selected vulnerabilities and threats along with their relative risk ratings (i.e., low, medium, high, and critical) and (iii) identified areas for review along with proposed corrective actions. The risk report also shows a "risk assessment rating key" showing "how [the] overall risk rating is calculated by combining threat likelihood with threat impact".[10]
- The "*remediation report*" is a report that provides (i) areas for review (along with proposed corrective actions) and (ii) text boxes to allow the organization to insert information on how to address proposed compliance gaps such as (a) the specific actions the organization will take to meet the recommendation, (b) the timeframe

[9] *See* SRA Tool User Guide at 31.
[10] *See* SRA Tool User Guide at 23.

to complete the proposed action, and (c) the responsible owner of the proposed action. The remediation report can therefore be used as a starting point for the covered entity's risk management plan.

- The "*detailed report*" provides all the information the organization provided in the assessment as well as all the information generated by the SRA Tool output.

All three reports above (i) indicate whether the proposed corrective actions are a "required" or "addressable" specification[11] under HIPAA and (ii) include the relevant section reference(s) corresponding to the corrective action under HIPAA, HITECH[12], and recognized security frameworks.[13]

Other features of the SRA Tool

The SRA Tool also allows organizations to (i) store information about their practice (e.g., the organization's departments, locations, and relevant persons) and (ii) track their IT assets and business associates, which can be exported out of the SRA Tool.[14]

RECENT OCR PENALTIES

Since October 2024, OCR has issued the following five (5) penalties against covered entities:

- On October 31, OCR announced it fined a community ambulance authority $90,000 for a violation of the Security Rule. The ambulance authority experienced a ransomware attack which led to a breach of ePHI. OCR cited to the community ambulance authority's failure to conduct a HIPAA required Risk Analysis. HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation for $90,000.

- On October 31, OCR announced it fined a plastic surgery association $500,000 for a violation of the Security Rule. The plastic surgery association was the victim of a ransomware attack which led to a breach of ePHI. The release states, "OCR's investigation revealed multiple potential violations of the HIPAA Security Rule, including failures to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems…" HHS Office for Civil Rights Settles Ransomware Cybersecurity Investigation for $500,000.

- On December 3, OCR announced it had fined a pain management clinic $1.19 million for a violation of the Security Rule. The pain management clinic experienced a breach of ePHI by a former contractor. In its release, OCR listed violations of the HIPAA security rule including failure to "conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems." HHS Office for Civil Rights Imposes a $1.19 Million Penalty Against Gulf Coast Pain Consultants for HIPAA Security Rule Violations.

---

[11] *See https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html* for information on the differences between a required and addressable specification under HIPAA.
[12] Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act, ARRA Public Law 111-5 Title XIII.
[13] Recognized security frameworks include: NIST Cybersecurity Framework 2.0, NIST Special Publications (800-66, 800-53, and 800-53A), the Health Industry Cybersecurity Practices (HICP) and the Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs).
[14] *See* SRA Tool User Guide at 12-17.

- On December 5, OCR announced it had fined a children's hospital $548,265 for a violation of the Security rule. The children's hospital experienced a phishing attack which led to a breach of ePHI. The release included that "OCR also found violations of the HIPAA Privacy Rule for failure to train workforce members on the HIPAA Privacy Rule, and the HIPAA Security Rule requirement to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems." HHS Office for Civil Rights Imposes a $548,265 Penalty Against Children's Hospital Colorado for HIPAA Privacy and Security Rules Violations.
- On December 10, OCR announced a settlement with a healthcare clearinghouse for $250,000. This was in addition to the healthcare clearinghouse's settlement with thirty-three (33) states that included corrective actions. This penalty was the result of an incident where ePHI held by the healthcare clearinghouse was available on public search engines, such as Google. In its release, OCR noted that its investigation "identified multiple potential HIPAA Security Rule violations including: failures by Inmediata to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems; and to monitor and review its health information systems' activity." HHS Office for Civil Rights Settles with Health Care Clearinghouse, Inmediata Health Group, Over HIPAA Impermissible Disclosure.

CONCLUSION

Due to OCR's recent blizzard of enforcement actions against organizations large and small, covered entities must prioritize HIPAA compliance. Specifically, covered entities must complete a HIPAA-compliant risk analysis and, if warranted, review and/or update previous risk analyses. Failure to meet this critical HIPAA requirement may subject cover entities to regulatory fines and potential reputational harm.

Sources

1. 45 C.F.R. §§ 164.306 - 164.316. *See* https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html for a complete set of all associated rules.
2. U.S. Department of Health and Human Services (HHS), *HIPAA Security Series 2 – Security Standards: Administrative Safeguards*, March 3, 2007, pp. 3-5 *("HIPAA Security Series 2")*.
3. U.S. Department of Health and Human Services (HHS), Guidance on Risk Analysis, *content last reviewed by OCR on July 22, 2019 ("OCR Risk Analysis Guidance")*.

ECKERT SEAMANS ATTORNEYS AT LAW